

1. General Information

Reference number	J010
Last update:	15/11/2018
Joint controllers:	EESC and CoR
Joint controllership arrangement	EESC-CoR JCA
Directorate/unit:	L2 INFRA
Contact details:	Directorate L Infrastructure Unit Rue Belliard, 99-101, 1040 Brussels
DPO - contact details	EESC Data Protection ; data.protection@cor.europa.eu
Processor(s)	Not applicable
Data Processing Agreement	Not applicable

2. Purpose and description of the personal data processing

Purpose(s) of the personal data processing	<p>In accordance with the rules laying down the provisions of the Economic and Social Committee and the Committee of the Regions, conditions relating to the preservation of all assets (except consumable goods and buildings) in line with Article 157 of the Financial Regulation (FR) and Article 247 of the Rules of Application (RAP), ABAC ASSETS 2 is the computerised system for managing the inventory of the Committees' assets.</p> <p>It includes all information relating to each item: inventory number, description, nomenclature code, department responsible, value of the item, delivery date, location, etc., as well as all the data required from an accounting perspective.</p>
--	--

	<p>It gives the option of indicating the name of the person professionally responsible for the item. This possibility is used in less than 1% of cases for items for personal use (such as medical furniture), but is essential for managing the inventory.</p> <p>Processing is necessary for the management and monitoring of all assets.</p>
Categories of persons whose personal data are processed	All staff occupying the Committees' buildings.
Categories of personal data processed	<ul style="list-style-type: none"> - User ID - surname - first name - office number - Committee.
Recipients of the personal data	<p>Only the CIS of the Infrastructure Unit, the verification services, the internal audit service and the accounting officers have access to all ABAC ASSETS data.</p> <p>The CRA, IT and Security and the managers of units purchasing goods have access to the data of their department only.</p> <p>Access is requested from the CIS by the head of unit and is forwarded to the Local Profile Manager (LPM) of the corresponding Committee, which will request DIGIT support.</p>
Transfers of personal data to a third country or an international organization	Not applicable
Retention period of the personal data	<p>The basic data are stored for the lifetime of the equipment in the inventory. Once the goods have been "written-off" or decommissioned, typically after a period of four to five years, the records on them are retained but users/assignees names are no longer accessible except under specific circumstances/conditions. (Historical information can only become accessible again after the re-activation of an item that was written off via administrative procedure - e.g. when a lost item which has been written off is found). Work is being considered to see if it is realistic to amend the system further to completely anonymise the retained data.</p>

General description of security measures, where possible	Access to the database is limited: only authorised persons have access to data relating to their department.
Data Protection Notice	Data Protection Notice available internally